Key Roles and Responsibilities

for

Information Risk Management

Authorizing Official

The *authorizing official* (or designated approving/accrediting authority as referred to by some agencies) is **a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. Through security accreditation, the authorizing official assumes responsibility and is accountable for the risks associated with operating an information system.** The authorizing official should have the authority to oversee the budget and business operations of the information system within the agency and is often called upon to approve system security requirements, system security plans, and memorandums of agreement and/or memorandums of understanding. In addition to authorizing operation of an information system, the authorizing official can also: (i) issue an interim authorization to operate the information system under specific terms and conditions; or (ii) deny authorization to operate the information system (or if the system is already operational, halt operations) if unacceptable security risks exist. With the increasing complexities of agency missions and organizations, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements should be established among the authorizing officials and documented in the system security plan. In most cases, it will be advantageous to agree to a lead authorizing official to represent the interests of the other authorizing officials. The authorizing official has inherent U.S. government authority and, as such, must be a government employee.

Senior Agency Information Security Officer (Information Security Manager, ISM)

The senior agency information security officer is the agency official **responsible for: (i) carrying out the Chief Information Officer responsibilities; (ii) possessing professional qualifications, including training and experience, required to administer the information security program functions; (iii) having information security duties as that official's primary duty; and (iv) heading an office with the mission and resources to assist in ensuring agency compliance with statutory and policy requirements.** The senior agency information security officer (or supporting staff member) may also serve as the authorizing official's designated representative. The senior agency information security officer **serves as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.**

Information Owner

The *information owner* is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. **The information owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations.** The owner of the

information stored within, processed by, or transmitted by an information system may or may not be the same as the information system owner. Also, a single information system may utilize information from multiple information owners. Information owners should provide input to information system owners regarding the security requirements and security controls for the information systems where the information resides.

Information System Owner

The *information system owner* is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The information system owner is **responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements.** The information system owner is also responsible for deciding who has access to the information system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). The information system owner informs key agency officials of the need to conduct a security certification and accreditation of the information system, ensures that appropriate resources are available for the effort, and provides the necessary system-related documentation to the certification agent. The information system owner receives the security assessment results from the certification agent. After taking appropriate steps to reduce or eliminate vulnerabilities, the information system owner assembles the security accreditation package and submits the package to the authorizing official or the authorizing official's designated representative for adjudication.

Information System Security Officer

The *information system security* officer is the individual **responsible** to the authorizing official, information system owner, or the senior agency information security officer **for ensuring the appropriate operational security posture is maintained for an information system or program**. The information system security officer also serves as the principal advisor to the authorizing official, information system owner, or senior agency information security officer on all matters (technical and otherwise) involving the security of the information system. The information system security officer typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many agencies, is assigned responsibility for the day-to-day security operations of the system. This responsibility may also include, but is not limited to, physical security, personnel security, incident handling, and security training and awareness. The information system security officer may be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis. In close coordination with the information system owner, the information system security officer often plays an active role in developing and updating the system security plan as well as in managing and controlling changes to the system and assessing the security impact of those changes.